Configurar a Integração de Tarefa Automática e Guarda-chuva

Contents

Introdução

Este documento descreve como configurar a integração do Autotask com o Umbrella.

Overview

A integração do Cisco Umbrella Autotask permite que os MSPs sejam notificados sobre terminais potencialmente infectados que exigem atenção criando automaticamente tickets no Autotask. A integração também envia dados de valor e status de implantação de serviço entre o Cisco Umbrella Dashboard e um produto instalado pelo Autotask Autotask (criado automaticamente) chamado "OpenDNS_Umbrella".

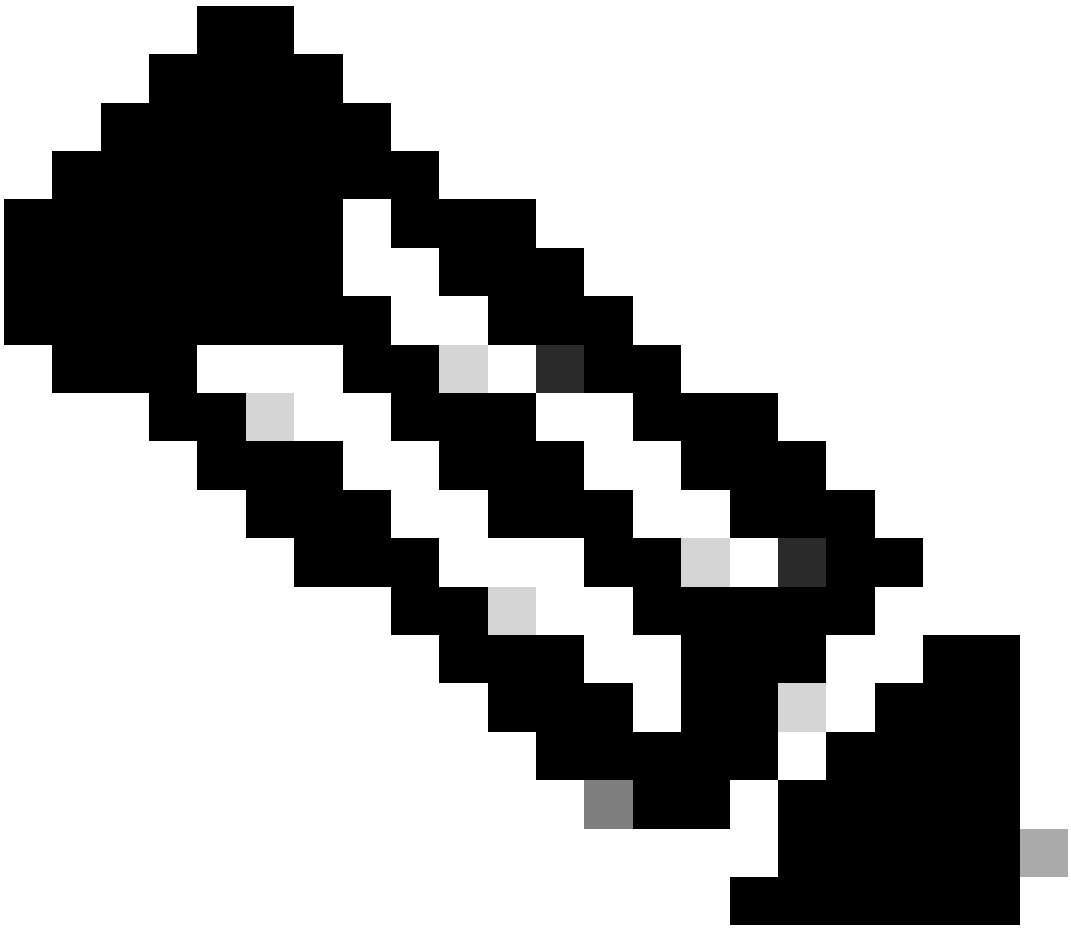
Etapas para a integração:

1. Pré-requisitos
2. Configuração inicial da autenticação de tarefa automática e do Cisco Umbrella
3. Configurar Tíquetes de Tarefa Automática
4. Mapeamento de empresas no Cisco Umbrella
5. Configurando o item de configuração "OpenDNS_Umbrella"

Pré-requisitos

Esta tabela contém os requisitos básicos de software para instalação:

Software	Versão	Modelo hospedado
Guarda-chuva da Cisco	Não aplicável	Hospedado
Tarefa automática	6.0 ou superior	Hospedado



Note: Somente uma (1) integração PSA pode ser adicionada por vez. Se você já tiver uma integração do Connectwise configurada, deverá excluí-la do painel para que a configuração da Tarefa automática possa continuar.

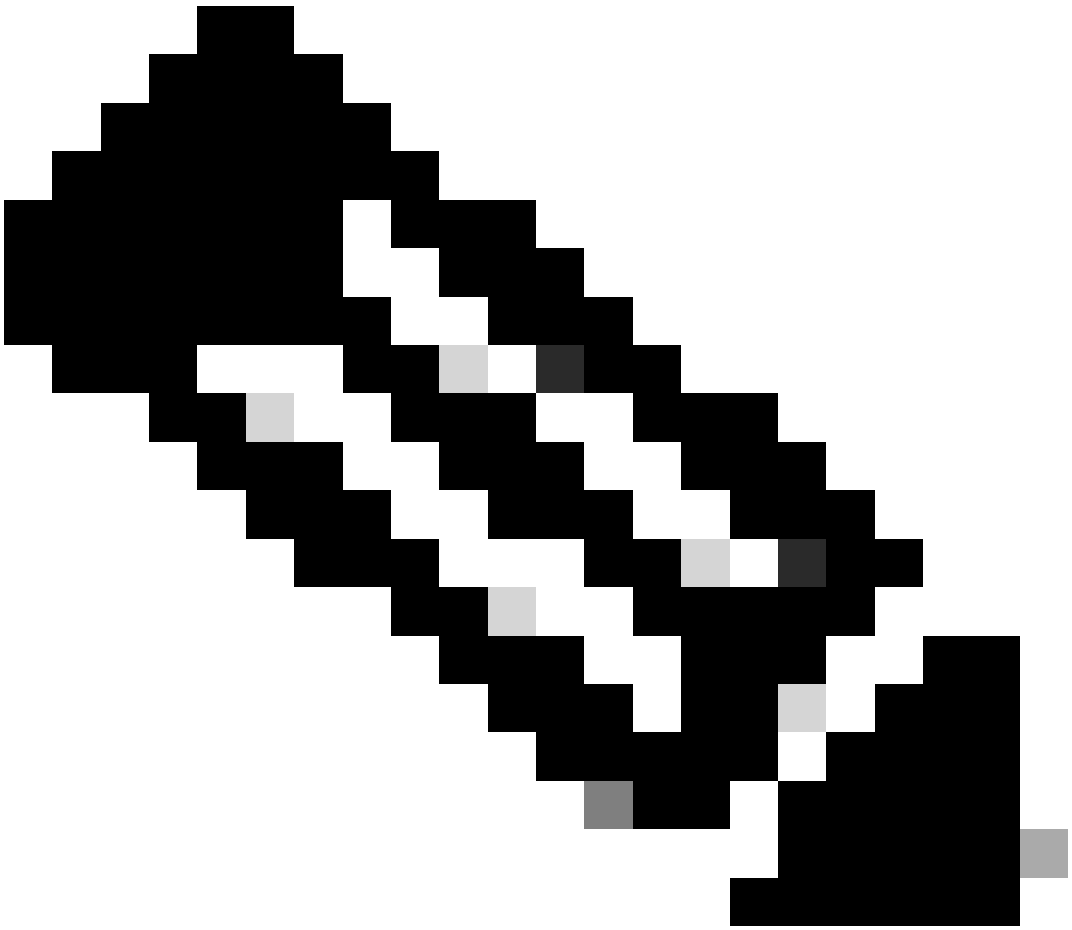
Configuração inicial da autenticação de tarefa automática e do

Cisco Umbrella

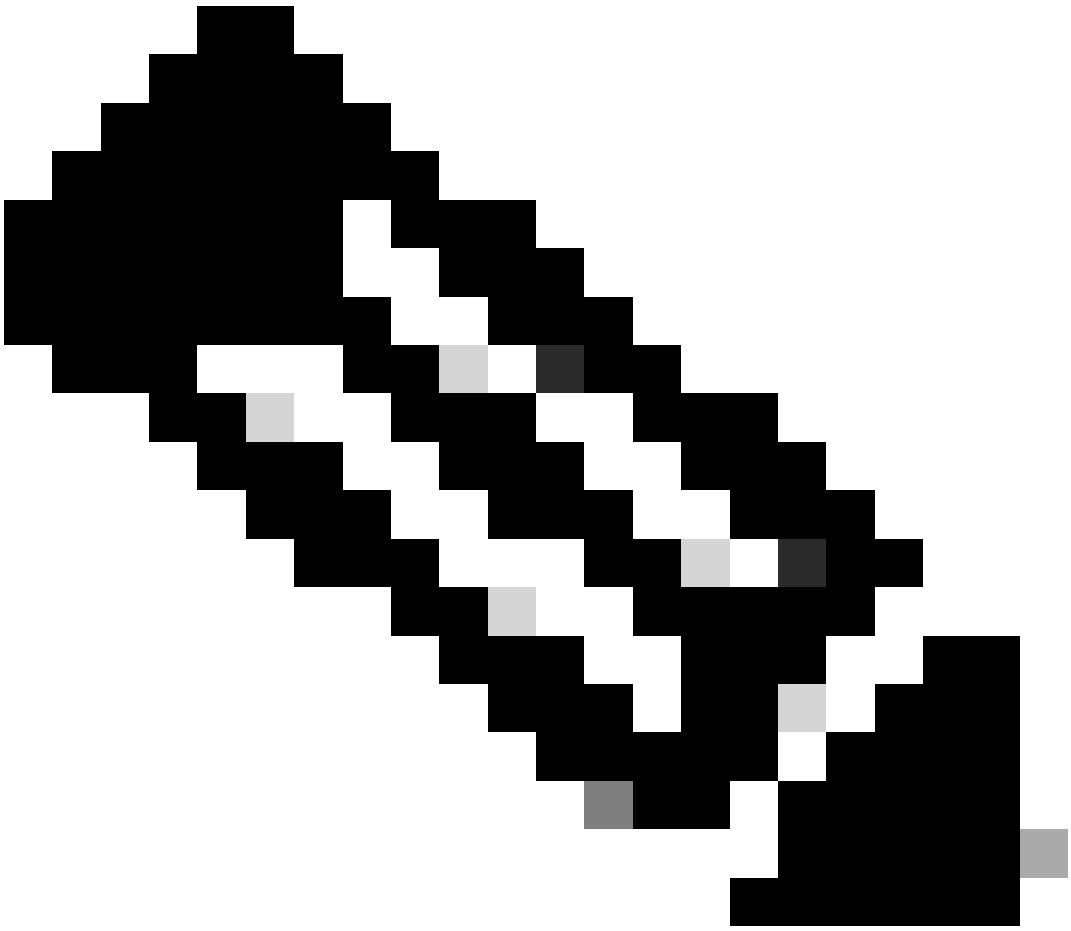
Estabelecer um usuário para autenticação:

Para se conectar à API do AutoTask, o Cisco Umbrella precisa de um login para o Autotask. Pode ser uma nova conta de recurso de usuário ou um logon compartilhado existente.

- Usuário existente: Se você já tiver um logon de Tarefa automática usado para integrações, verifique se a conta está definida como um Usuário de API. A conta não deve usar autenticação em duas etapas.
- Novo usuário: Para criar um novo recurso de usuário:
  - Faça login no painel do Autotask.
  - Selecione Admin **>** CiscoResources (Users) **>** New.
  - Preencha os requisitos de informações pessoais do usuário nas guias HR.
  - Na guia Security, verifique se o nível de segurança desse usuário está definido como "API User (system)".



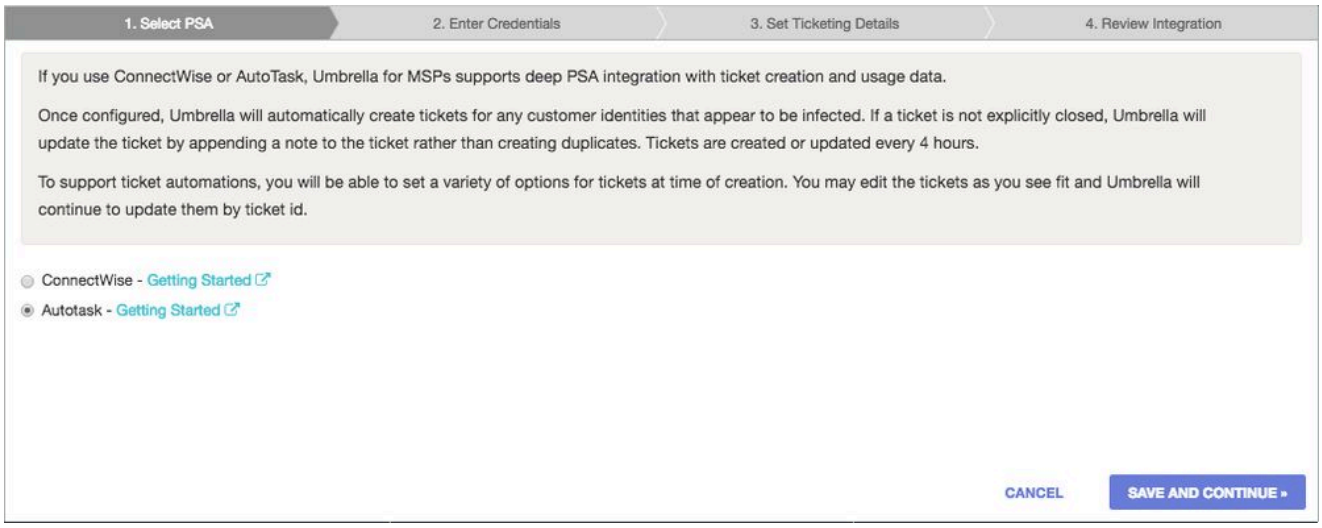
Note: O usuário para autenticação deve ter a caixa de seleção "Exibir dados desprotegidos" marcada em Admin > Recursos e configurações > Recursos/usuários (RH) > Segurança > Permissão de dados protegidos > [o usuário para autenticação].



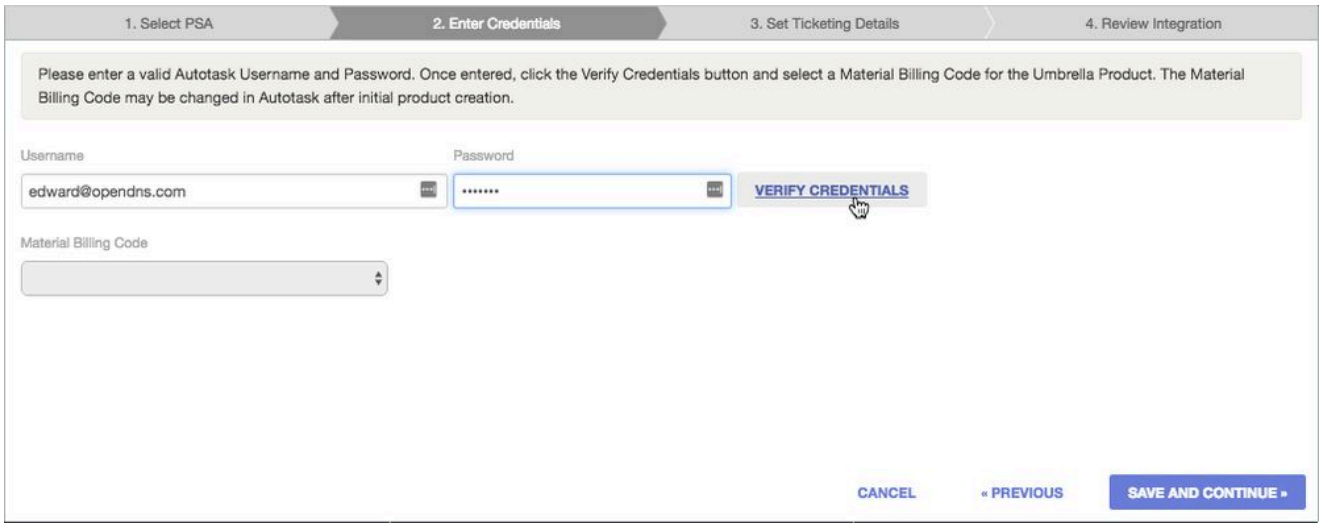
Note: A partir de 1º de junho de 2021, o usuário de autenticação deverá ter um identificador de rastreamento de API definido. Para obter mais informações, consulte este artigo da Base de conhecimento Umbrella: Mudanças na integração do Autotask PSA com o Umbrella

Depois que uma conta for criada ou selecionada, navegue até o Umbrella para MSPs.

1. Navegue até Configurações de MSP > Detalhes de integração de PSA.
2. Selecione Configurar integração para abrir o assistente de integração.
3. Em Select PSA, selecione Autotask como o tipo de integração e, em seguida, selecione Save and Continue.



4. Em seguida, você será solicitado a inserir a conta selecionada anteriormente (endereço de e-mail e senha) e verificar suas credenciais para selecionar um Código de faturamento de material:



Selecione o Código de Faturamento de Material apropriado:

Depois de autenticado, o Código de Faturamento de Material mostra uma seleção com seu código de faturamento de material de Tarefa Automática existente. Posteriormente, você poderá alterar o código de cobrança do material para o produto "OpenDNS_Umbrella" no Autotask, se desejar.

Selecione Salvar e continuar.

Configurar Tíquetes de Tarefa Automática

O Cisco Umbrella para MSPs notifica proativamente sobre hosts infectados que exigem ação criando tickets dentro de uma fila de Central de serviços de tarefa automática. Quando integrado corretamente, o Cisco Umbrella verifica automaticamente se há hosts infectados e cria tickets para você.

Como um tíquete de fila de serviço é gerado pelo Cisco Umbrella:

No momento, esses critérios devem ser atendidos para gerar um ticket dentro de uma fila da Central de serviços de tarefa automática:

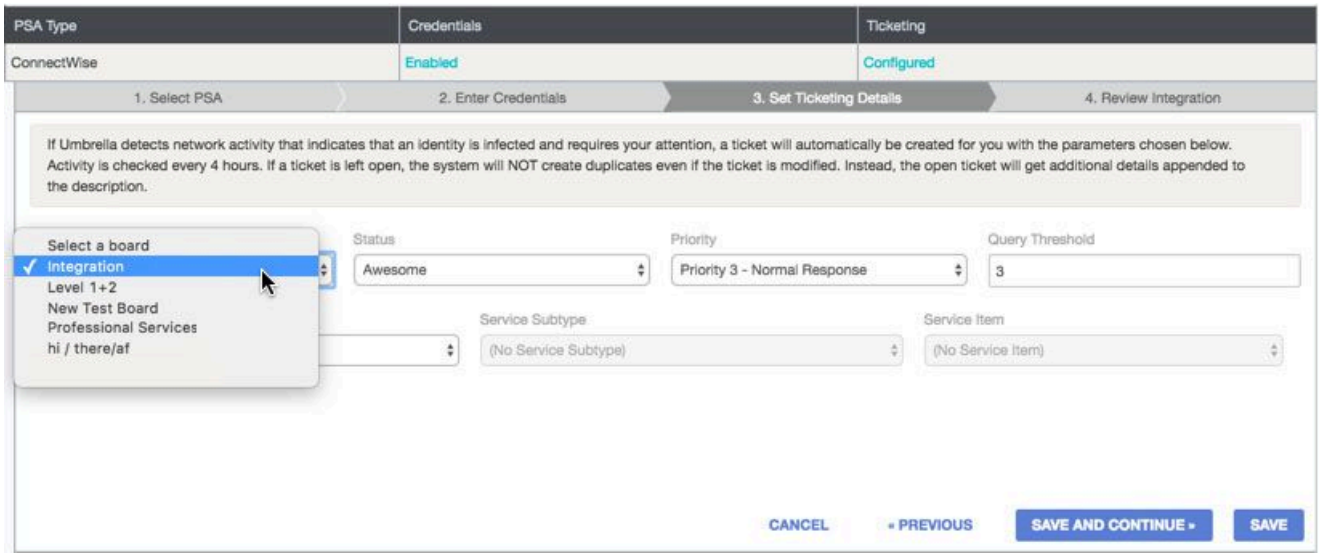
- O Cisco Umbrella monitora suas identidades quanto ao bloqueio de "atividades de botnet". Esta atividade indica um endpoint que está infectado e que o Cisco Umbrella está bloqueando ativamente as tentativas de "ligar para casa" para atualizações, carregar dados roubados ou fazer parte de um botnet. Se uma identidade em sua organização estiver tentando repetidamente acessar um site categorizado como "botnet". Isso significa que, embora o Cisco Umbrella esteja contendo o dano, a máquina está infectada com malware e precisa de ação adicional de sua parte para a correção.
- O Cisco Umbrella não cria alertas quando evita infecções para categorias como malware ou downloads drive-by, pois esses eventos impedem preventivamente o usuário de visitar sites mal-intencionados. Nenhuma ação adicional é necessária.
- A cada quatro horas, o Cisco Umbrella verifica todas as organizações mapeadas para organizações PSA no console Cisco Umbrella for MSP.
- Se uma única identidade, como um computador com um agente instalado ou uma rede, tiver mais eventos de botnet do que o "limite de consulta" (três por padrão) dentro do bloco de quatro horas, o Cisco Umbrella Integration abrirá automaticamente um ticket dentro do Service Desk definido pelo Ticketing Details Integration no assistente de integração. Você pode alterar o limite de consultas aqui.
- Se a mesma identidade continuar a gerar atividade adicional de botnet na próxima janela de quatro horas (ou outra janela de tempo depois disso) e o ticket ainda estiver aberto, dados adicionais serão anexados ao ticket.
    - O Cisco Umbrella faz referência ao ticket pelo seu número de ticket e não cria duplicatas desnecessárias, mesmo se um ticket for movido para outra fila do Service Desk ou se a cópia for alterada.
- Se o tíquete tiver sido marcado como Fechado, um novo tíquete será criado, pois presume-se que esse seja um novo evento de segurança relacionado a botnet (como uma nova infecção) para a mesma identidade.

Definir detalhes do tíquete:

Se estiver usando o Assistente de integração, você estará na etapa 3 do Assistente de integração. Se estiver configurando a emissão de tíquetes mais tarde, selecione Integração PSA > Detalhes da integração.Suas credenciais agora são mostradas como habilitadas, mas a emissão de tíquetes é desabilitada.

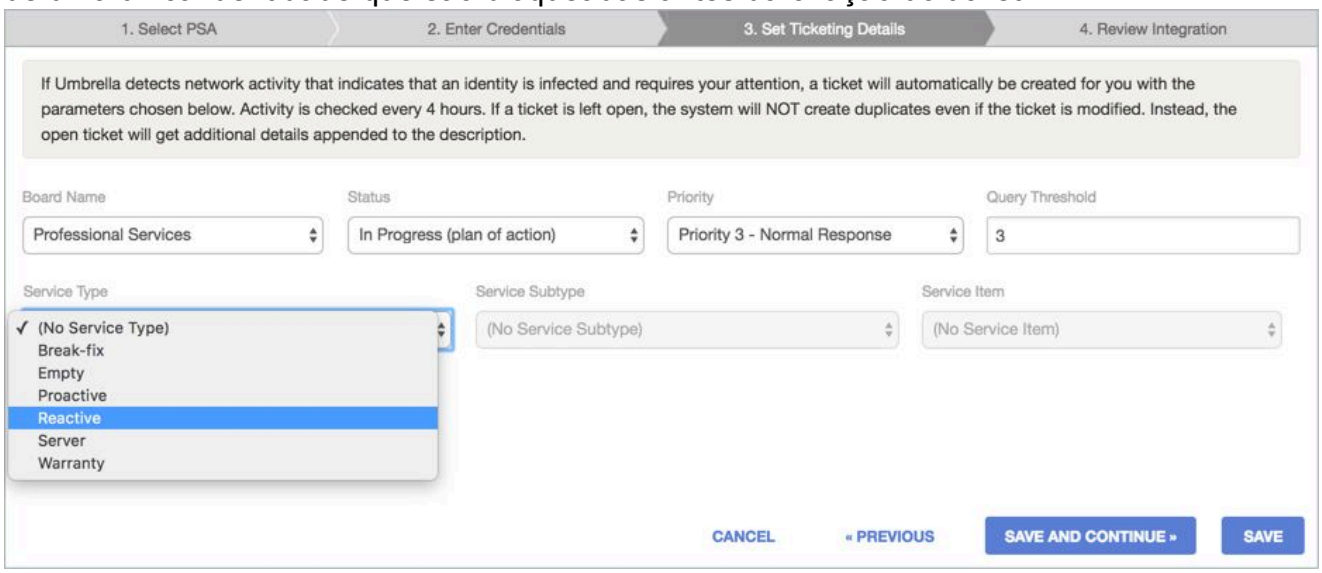
1. Ao selecionar Tíquetes > Desativado, você será levado para Definir detalhes de tíquetes.

2. Primeiro, selecione uma fila. Este exemplo usa a fila Triagem para deixar tíquetes. Você deve selecionar a fila primeiro para preencher os campos adicionais:



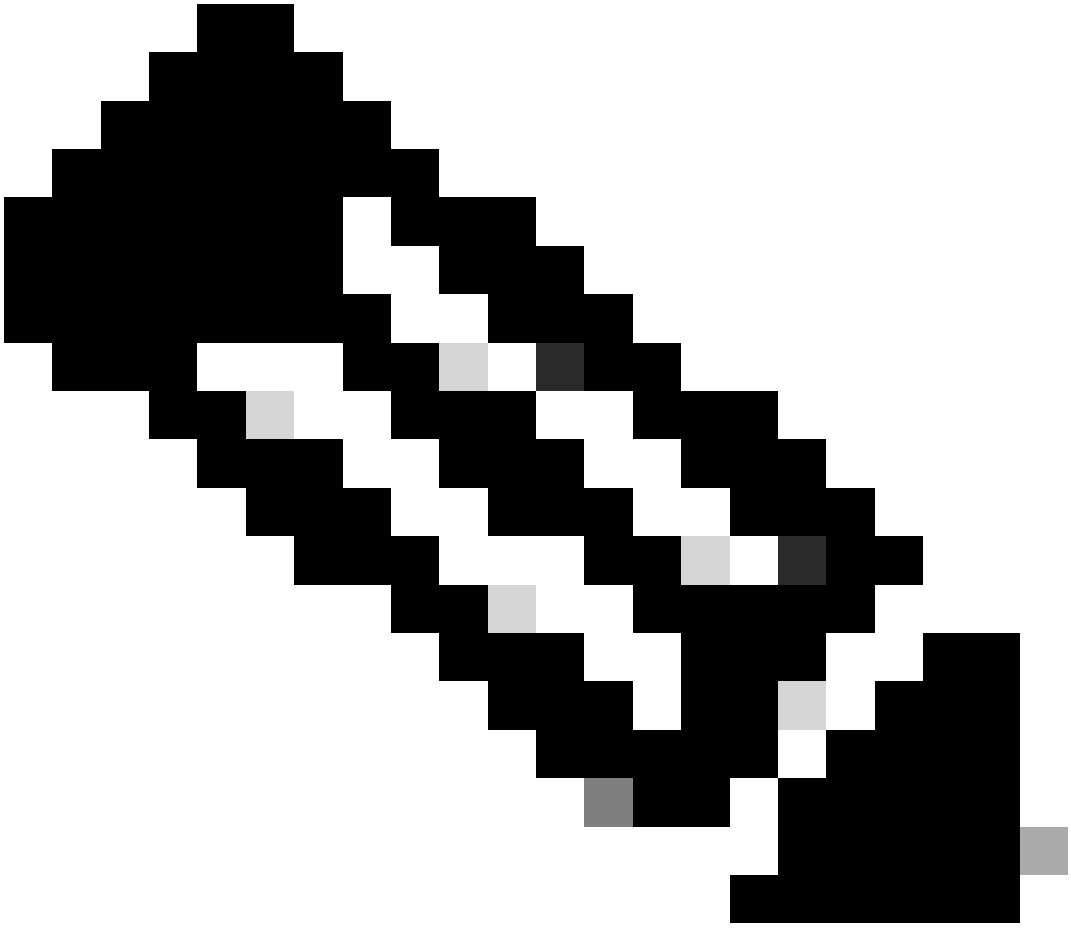
215690567

3. Depois de selecionar a fila, aguarde alguns segundos para que o detalhe seja preenchido para os campos restantes e, em seguida, selecione o apropriado. Cada campo no Cisco Umbrella Dashboard é mapeado para o campo equivalente nos tíquetes da fila da Central de serviços selecionada.
   Os parâmetros exatos para cada campo variam levemente com base na implementação. Um campo de observação é o Limite de consulta, que é o número de atividades de botnet de uma única identidade que são bloqueadas antes da criação do ticket.



4. Preencha todos os campos conforme aplicável e selecione Salvar e continuar.

A quarta e última etapa da integração permite que você revise todas as suas configurações para garantir que elas sejam o que você espera.



Note: Se quiser gerar um tíquete de teste, entre em contato com o Suporte do Cisco Umbrella e solicite a geração. Esse ticket obedece às suas regras de tíquete de Tarefa automática.

Mapeamento de empresas no Cisco Umbrella

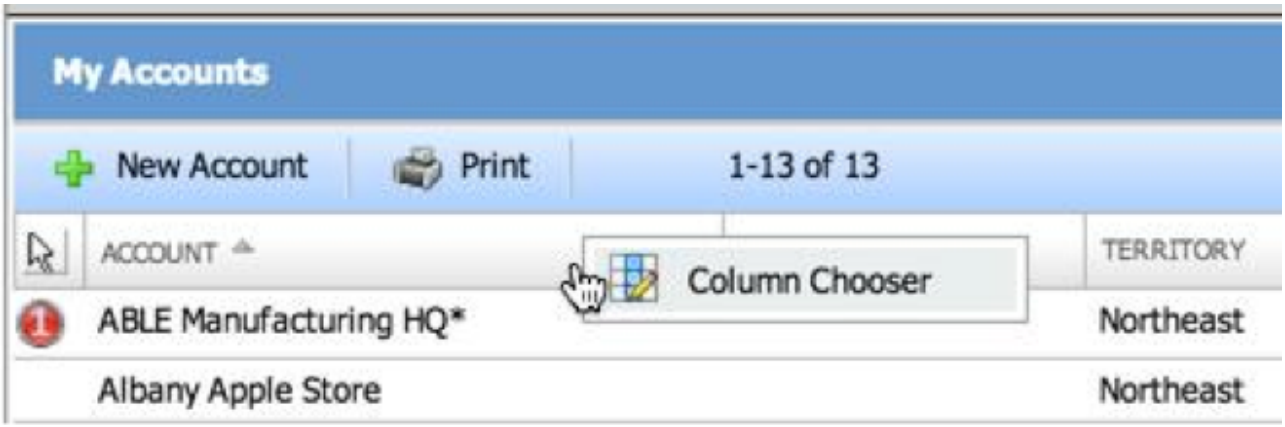
O mapeamento de empresas do cliente permite a integração e permite que tíquetes e produtos instalados sejam associados à conta do cliente. O produto instalado "OpenDNS_Umbrella" contém estatísticas valiosas sobre o uso e a eficácia do Cisco Umbrella pelo cliente e é configurado na Etapa 5.

Para sincronizar clientes entre o Autotask e o Cisco Umbrella, você deve ter a ID da conta para cada cliente. Isso não é mostrado na Tarefa automática por padrão.

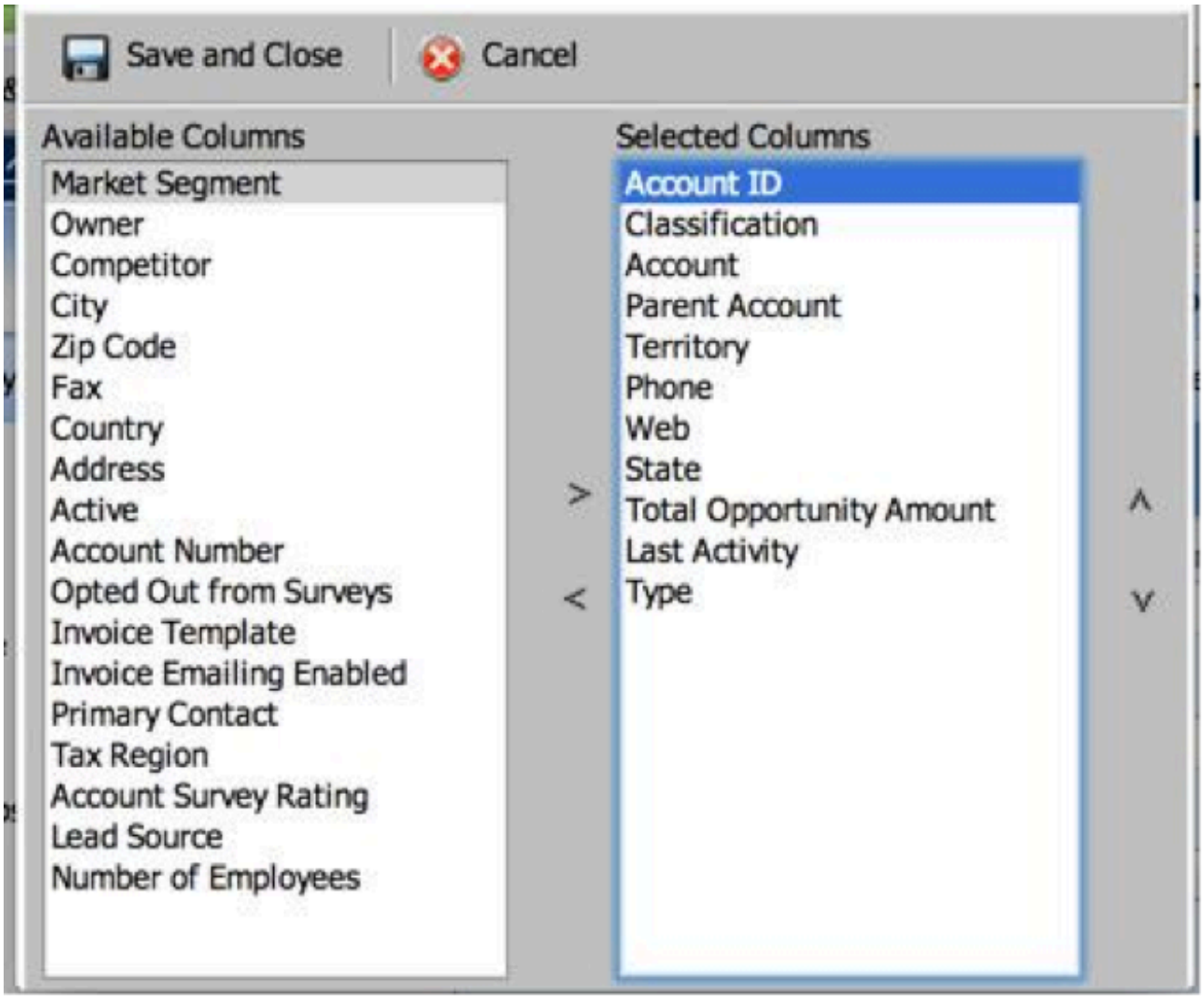
1. Para ver a ID do cliente no painel de tarefas automáticas, selecione CRM e escolha Minhas contas na lista suspensa. Cada conta tem uma ID de conta nas propriedades dessa conta visível clicando duas vezes no nome da conta, o que abre uma janela pop-up que mostra a

ID da conta.

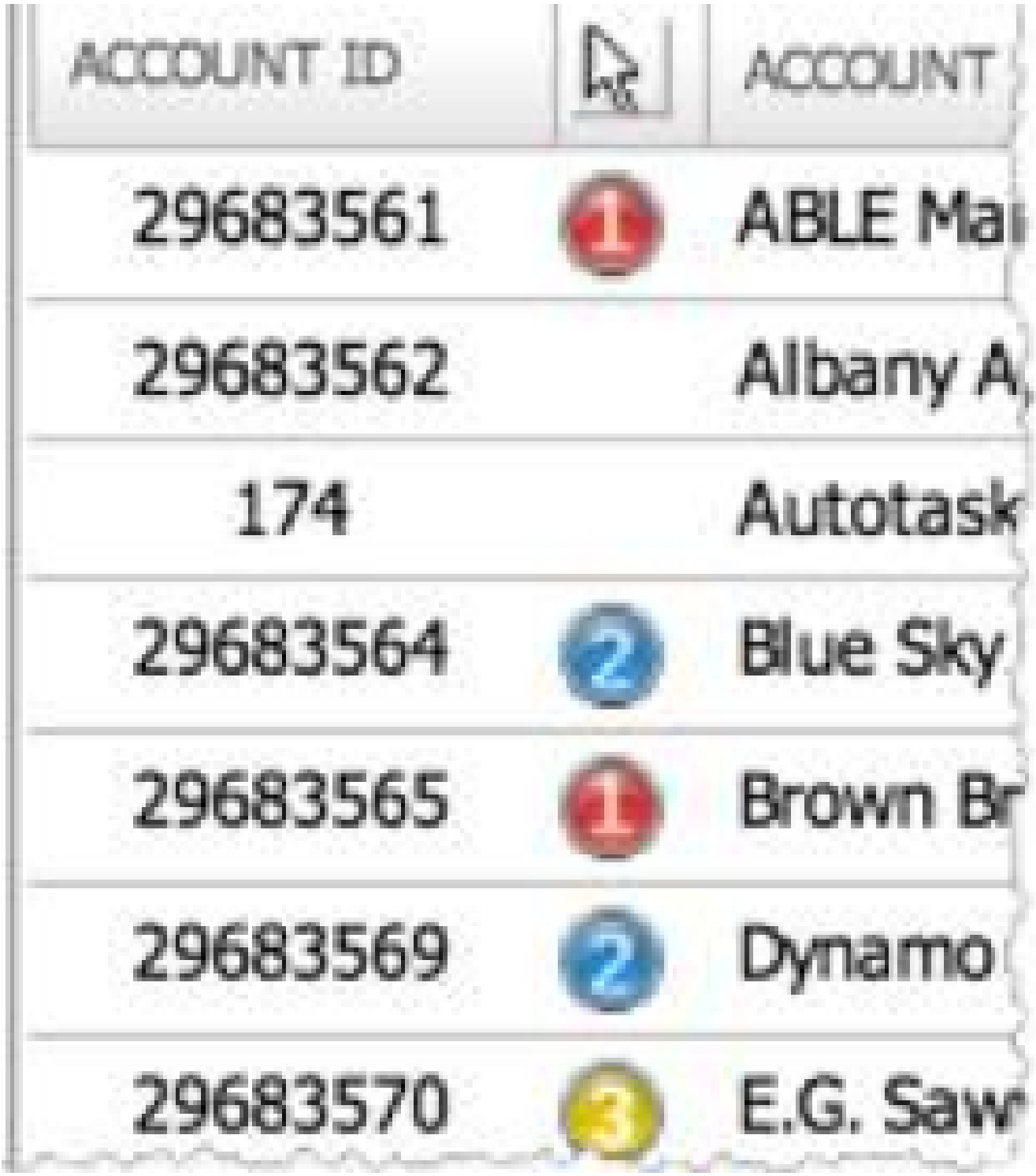
2. Para ver todas as IDs de conta de seus clientes na visão geral, você deve expor uma nova coluna. Clique com o botão direito do mouse nas colunas para mostrar o Seletor de Colunas.



3. No seletor de colunas, mova a coluna ID da conta para Colunas selecionadas.

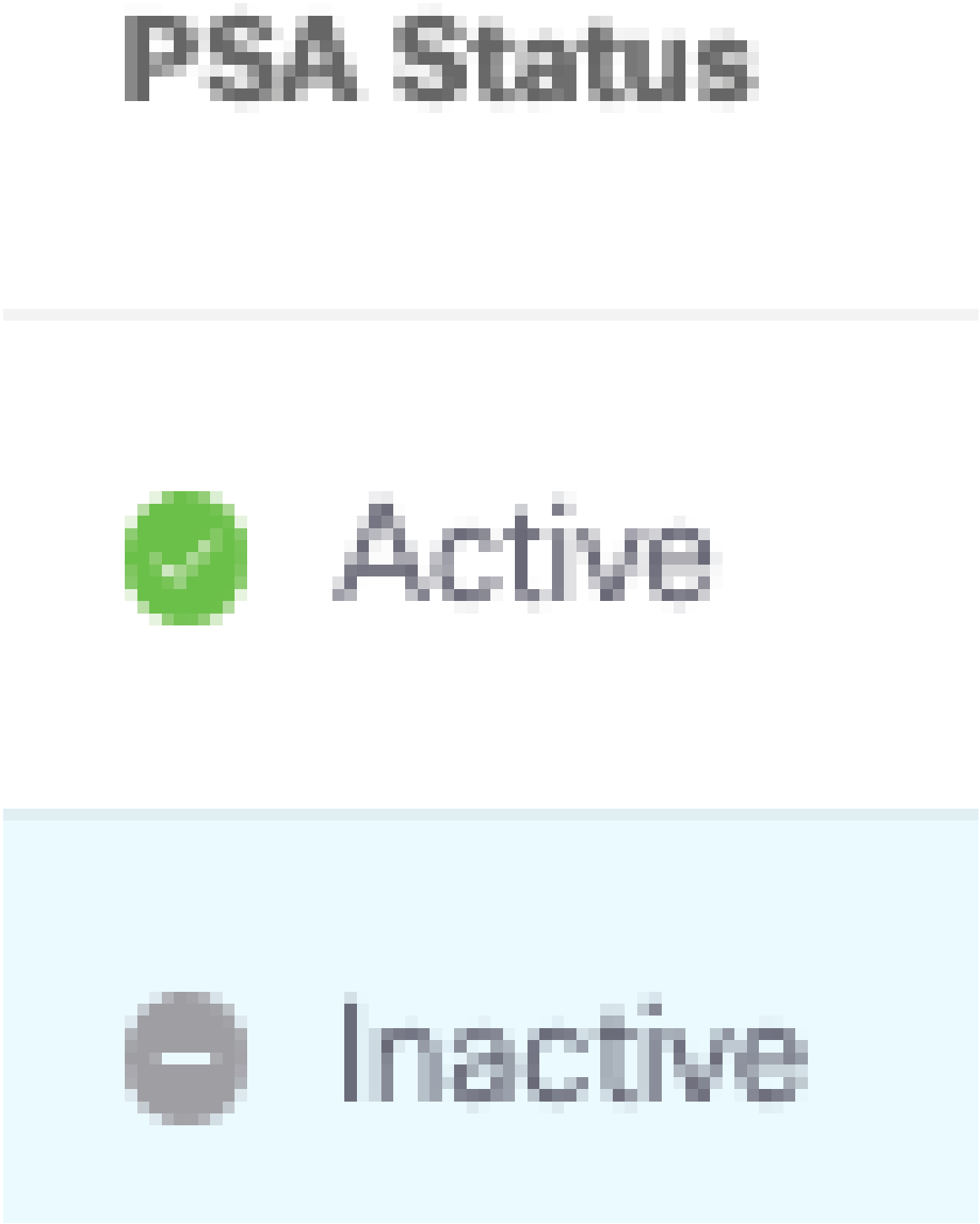


Mostra a ID da conta do cliente:



4. Quando tiver a ID da conta do cliente, retorne ao Cisco Umbrella para MSPs.
5. Navegue até Gerenciamento de clientes para mostrar uma lista dos clientes que você configurou em seu console
   Note: Se não houver clientes listados aqui, você precisará adicionar clientes ao MSP do Cisco Umbrella para MSPs. Leia o Guia do usuário do Cisco Umbrella para MSPs para obter mais informações.
6. Em seguida, selecione o cliente a ser mapeado para a Tarefa automática. Este exemplo usa "Able Manufacturing Co."
7. Antes, descobrimos que a Able Manufacturing Co. tem uma ID de conta igual a 29683561. Selecione o nome do cliente e insira a ID da conta da empresa no campo da ID do PSA.

8. Selecione Save para confirmar a alteração. Você recebe uma mensagem de confirmação sobre a integração que está sendo ativada. Desse ponto em diante, a ID do PSA é exibida ao lado do cliente para o qual está habilitada em Detalhes do cliente.
9. Para confirmar se a integração está habilitada, navegue até Relatórios centralizados > Status de implantação. Se estiver operacional, uma coluna PSA Status será preenchida.
    - As organizações com IDs PSA válidas aparecem com um status Ativo verde.
    - As organizações que não têm um valor de ID de PSA aparecem com um status Inativo cinza.



360053576152

Configuração do item de configuração "OpenDNS_Umbrella" (opcional)

Depois que a ID da empresa PSA tiver sido integrada com êxito, um item de produto/configuração instalado chamado OpenDNS_Umbrella será criado automaticamente.

Você pode exibir o Item de configuração em Diretório > Contas e selecionar uma das contas integradas na Etapa 4. Nessa conta, agora há um Item de configuração para OpenDNS_Umbrella.

Observe que, por padrão, o Item de configuração inclui todos os campos possíveis e os campos do Cisco Umbrella que adicionamos na integração. Alguns campos não são preenchidos porque não se aplicam ao Cisco Umbrella, como Marca ou Marca e Modelo.

Para alterar o produto de forma a não incluir esses campos, defina um tipo de configuração exclusivo para o Cisco Umbrella.

Instalação do tipo de configuração

Os itens de configuração criados em Tarefa automática através da integração do Cisco Umbrella criam campos definidos pelo usuário (UDFs) para suas informações de atualização automática do Cisco Umbrella. Por padrão, um novo produto mostra todos os UDFs, e um tipo de item de configuração é recomendado. Devido a limitações com a API de Tarefa Automática atual, a criação de um Tipo de Item de Configuração dentro da Tarefa Automática está limitada à intervenção manual por você ou pelo administrador da Tarefa Automática. Esta tabela fornece uma lista de todos os campos que devem ser adicionados ao Tipo de item de configuração.

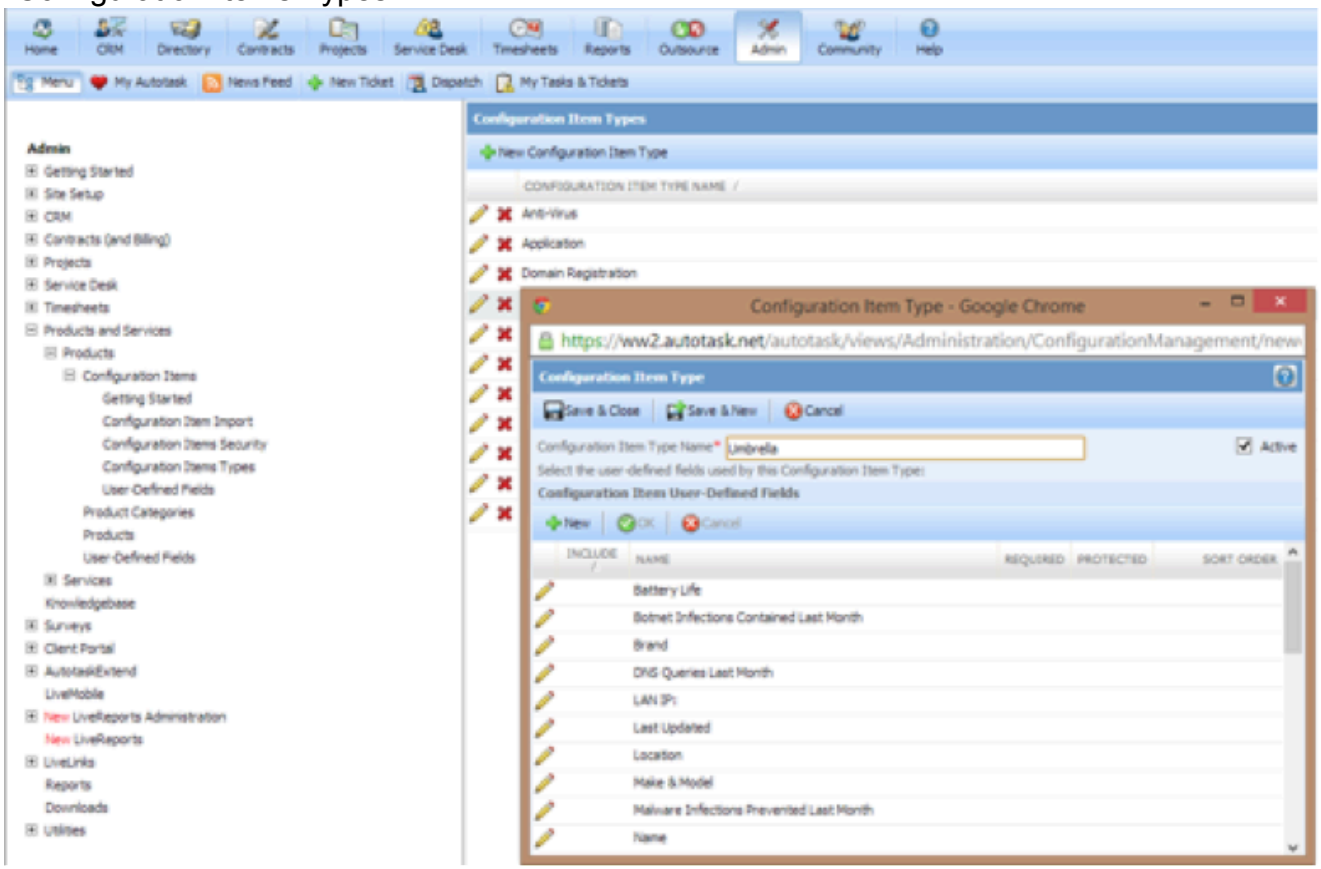
#	Nome do campo	Tipo
1	ID da Organização	Texto (linha única)
2	Última atualização	Texto (linha única)
3	Pacote	Texto (linha única)
4	Assentos	Texto (linha única)

5	Total de Redes	Texto (linha única)
6	Redes Ativas nos Últimos 7 Dias	Texto (linha única)
7	Redes Inativas nos Últimos 7 Dias	Texto (Várias Linhas)
8	Agentes Umbrella implantados	Texto (linha única)
9	Agentes Umbrella ativos nos últimos 7 dias	Texto (linha única)
10	Agentes Umbrella inativos nos últimos 7 dias	Texto (Várias Linhas)
11	Consultas DNS no mês passado	Texto (linha única)
12	Infecções por malware evitadas no mês passado	Texto (linha única)
13	Infecções pelo Botnet Contidas no Mês Passado	Texto (linha única)
14	Principais domínios no mês passado	Texto (Várias Linhas)
15	Principais domínios bloqueados no mês passado	Texto (Várias Linhas)

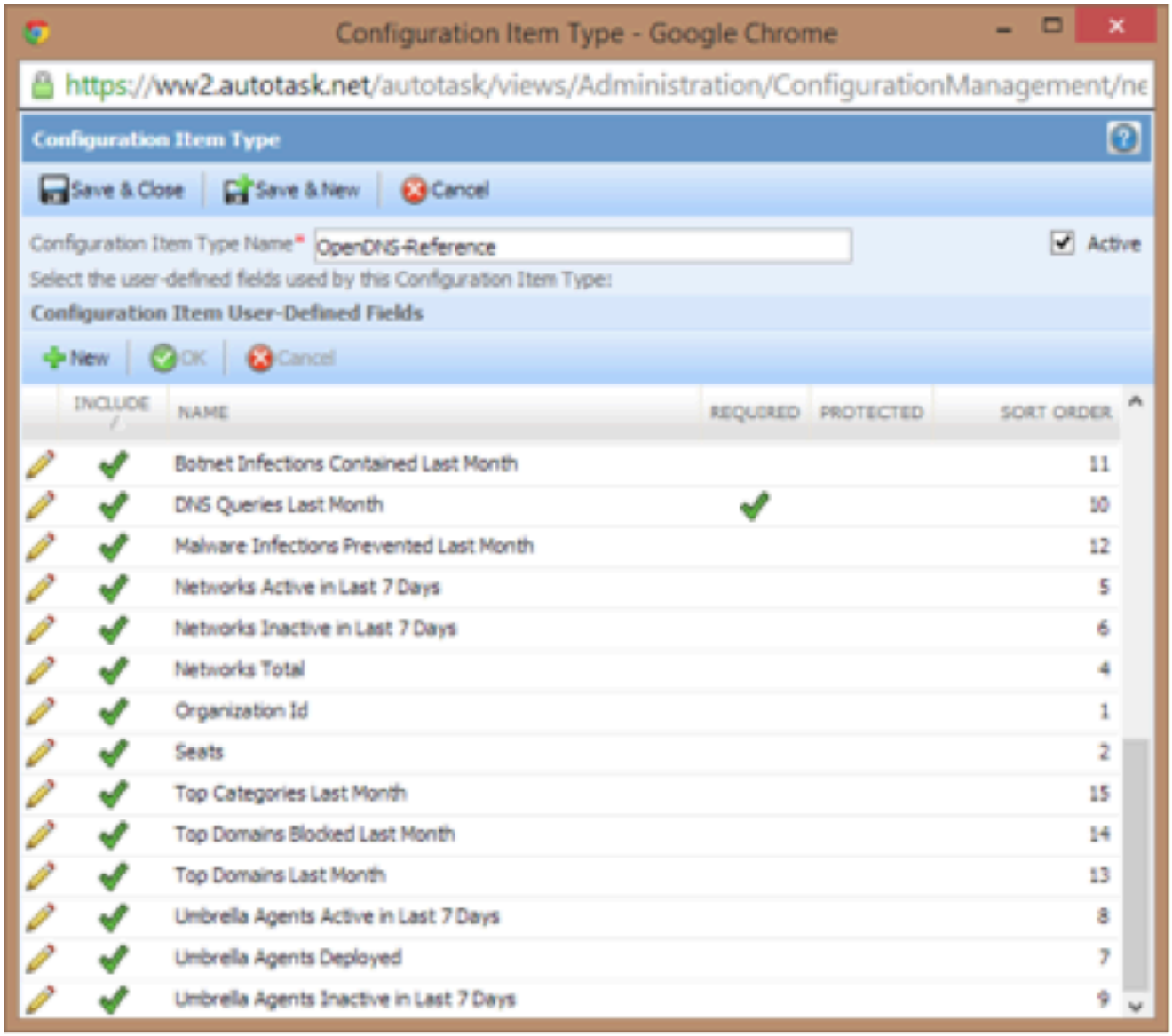
16	Principais categorias no mês passado	Texto (Várias Linhas)

Para usuários que não estão familiarizados com a configuração de novos Tipos de item de configuração em Tarefa automática, use estas instruções para criar o novo registro no sistema:

1. Entre no Autotask como administrador.
2. Navegue até a seção Admin usando o menu superior.
3. Navegue até Products and Services > Products > Configuration Items e selecione "Configuration Items Types".

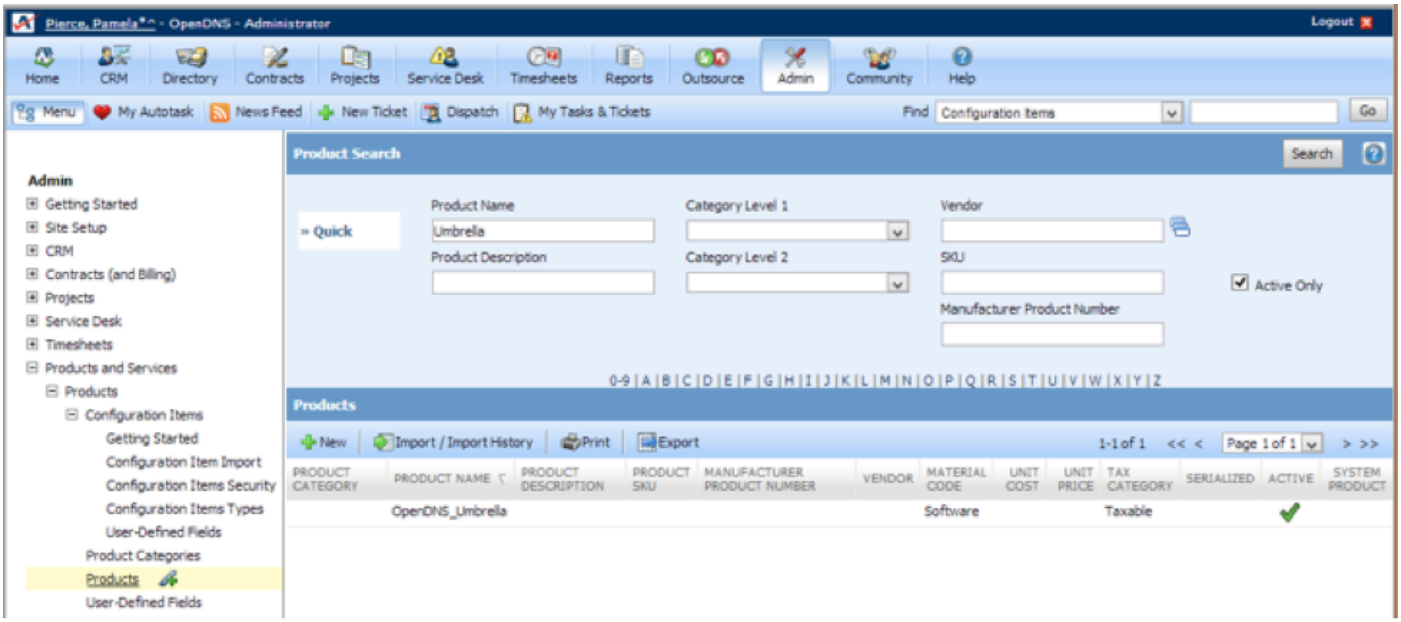


4. Selecione a opção de menu Novo tipo de item de configuração.
5. Digite um nome para o novo Tipo de item de configuração.
6. Selecione New e insira as informações do campo para o primeiro campo na parte superior.
7. Repita a etapa 6 até ter adicionado todos os campos da tabela ao novo tipo de item.



8. Salve e feche o novo Tipo de Item de Configuração.

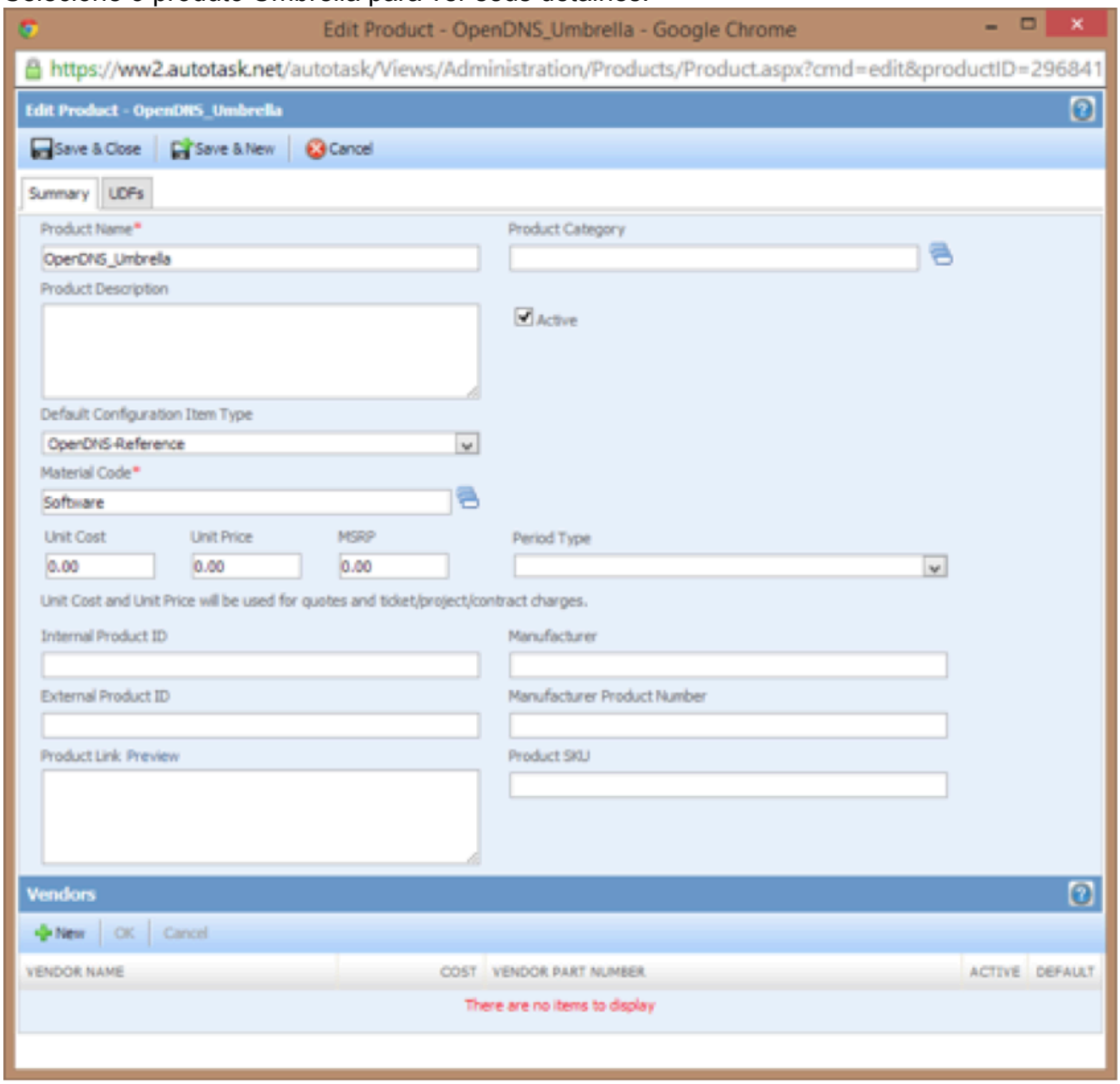
Configuração do produto



A integração com o Cisco Umbrella cria automaticamente um Produto na implementação da Tarefa automática para vincular itens de configuração ao momento da criação. Depois que o produto tiver sido criado no sistema, o Cisco Umbrella recomenda que você atualize a definição do produto com as configurações que melhor reflitam seus padrões e necessidades comerciais.

Para identificar a definição do produto e atualizar suas configurações, siga estas etapas:

1. Entre no Autotask como administrador.
2. Navegue até a seção Admin usando o menu superior.
3. Navegue até Products and Services > Products e selecione Products.
4. Digite "Umbrella" no campo de pesquisa Nome do produto e selecione Pesquisar.
5. Selecione o produto Umbrella para ver seus detalhes.



6. Atualize a definição do produto para refletir as configurações desejadas.
7. Selecione Save & Close.

Notas:

- Não altere a string do nome do produto de "OpenDNS_Umbrella" para outra coisa. Isso interrompe a integração, mas se você a renomeou, renomeie-a novamente para corrigir o problema.
- Certifique-se de que "Ative: está selecionado como você vê na captura de tela.

As definições de cada um dos campos do Cisco Umbrella AutoTask que são atualizados e incluídos no Item de configuração estão listados nesta tabela:

Campo	Descrição
ID da Organização	ID da organização interna do guarda-chuva
Última atualização	Data em que a última sincronização com o Umbrella ocorreu
Assentos	Número total de estações aplicadas a esta empresa.
Total de Redes	Número total de redes aplicadas a esta empresa
Redes Ativas (7 Dias)	Número total de redes ativas nos últimos sete dias
Redes Inativas (7 Dias)	Lista de nomes de rede inativos nos últimos sete dias
Agentes Umbrella implantados	Número de agentes Umbrella Roaming implantados
Agentes Umbrella Ativos 7 Dias	Número de agentes de roaming Umbrella ativos nos últimos sete dias

Agentes Umbrella Inativos 7 Dias	Nomes das identidades dos agentes de roaming do Umbrella inativas nos últimos sete dias
Consultas DNS no mês passado	Número total de solicitações DNS para esta empresa no mês do calendário anterior
Infecções por malware evitadas no mês passado	Número de sites que hospedam malware impedidos de acessar no mês anterior
Infecções pelo Botnet Contidas no Mês Passado	Número de sites que hospedam comando e controle de botnet impedidos de acessar no mês anterior
Principais domínios no mês passado	Lista dos nomes dos domínios mais acessados no mês anterior
Principais domínios bloqueados no mês passado	Lista dos nomes dos domínios bloqueados com mais frequência no mês do calendário anterior
Principais categorias no mês passado	Lista das categorias de conteúdo solicitadas com mais frequência no mês anterior, incluindo o número de solicitações por categoria

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.